WE CLAIM:

1. A method for distributed network address translation with security, comprising the following steps:

providing a first network device and a second network device on a first network;

establishing a security association between the first network device and a third network device on a second network external to the first network;

specifying an external address of the third network device for the security association;

storing the external address in a table on the second network device; and

mapping at least one of an internal address and a security value to the external address in the table.

2. A computer readable medium having stored therein instructions for causing a central processing unit to execute the method of claim 1.

3. The method of claim 1 wherein the second network device is a distributed network address translation router.

4. The method of claim 1 wherein the security value is a security parameter index for an Internet Protocol security protocol.

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

5. The method of claim 4 wherein the Internet Protocol security protocol is any of an Authentication Header protocol, Encapsulated Security Payload protocol, or an Internet Key Exchange protocol.

6. The method of claim 1 further comprising the step of specifying the external address of the third network device for the security association with a Port Allocation Protocol external address validating message sent from the first network device to the second network device.

7. The method of claim 6 wherein the Port Allocation Protocol external address validating message has a valid external address field.

8. The method of claim 1 further comprising the step of removing the external address from the table with a Port Allocation Protocol external address invalidating message sent from the first network device to the second network device.

9. The method of claim 8 wherein the Port Allocation Protocol external address invalidating message has an invalid external address field.

10. A method for distributed network address translation with security, comprising the following steps:

providing a first network device and a second network device on a first network, and a third network device on a second network external to the first network;

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

sending a packet having an external address and a security value from the third network device to the first network device;

intercepting the packet with the second network device;

determining whether the security value of the packet has been allocated to the first network device;

determining whether the external address of the packet has been specified by the first network device as being valid; and

sending the packet from the second network device to the first network device if the security value has been allocated to the first network device and the external address of the packet has been specified by the first network device as valid.

11. A computer readable medium having stored therein instructions for causing a central processing unit to execute the method of claim 10.

12. The method of claim 10 wherein the second network device is a distributed network address translation router.

13. The method of claim 10 wherein the security value is a security parameter index for an Internet Protocol security protocol.

14. The method of claim 13 wherein the Internet Protocol security protocol is either an Authentication Header protocol or an Encapsulated Security Payload protocol.

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

15. The method of claim 10 further comprising the step of discarding the packet if the security value of the packet has not been allocated to the first network device.

16. The method of claim 10 further comprising the step of discarding the packet if the external address of the packet has not been specified by the first network device as being valid.

17. The method of claim 10 further comprising the steps of discarding the packet if the security value of the packet has not been allocated to the first network device, and discarding the packet if the external address of the packet has not been specified by the first network device as being valid.

18. The method of claim 10 further comprising the step of specifying the external address as being valid if a security association has been established between the first network device and the third network device.

19. The method of claim 18 further comprising the step of storing a valid external address in a table on the second network device.

20. A system for distributed network address translation with security comprising:

a routing network device using distributed network address translation with security to provide routing services for a plurality of internal and external network devices; and

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

an established security association table associated with the routing network device for storing external addresses of external network devices that have established security associations with internal network devices, and mapping external addresses that have been specified as valid by the internal network devices to one of internal network addresses and security values for established security associations.

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001